Remarks

Applicant responds herein to each of the issues raised in the Office Action mailed December 16, 2004. The Office Action acknowledges that Claims 7-13, 17-19, 29, 30, 36 and 43 contain patentable subject matter. However, Applicant has not amended these claims to place them in a form indicated as allowable at this time as Applicant submits the rejected claims are also allowable for the reasons discussed below.

Claims 1-6, 14-16, 20-28, 31-35, 37-42 and 44-46 stand rejected under 35 U.S.C. § 103 as being unpatentable over Gennaro *et al.*, "How to Sign Digital Streams" (hereinafter "Gennaro") in view of "Introduction to Distributed Memory Programming" (hereinafter "CSU") and Wagner *et al.*, "Analysis of the SSL 3.0 Protocol" (hereinafter "Wagner"). Office Action, p. 2. Applicant submits that the rejection should be withdrawn at least as none of the cited references disclose the use of a group MAC wherein individual communication packets "do not incude an associated packet MAC" as recited in Claim 1.

The present invention is generally directed to message authentication for SSL-based protocol connections where a group message authentication code (MAC) is used instead of individual packet associated packet MACs. As such, SSL protocol bottleneck problems may be reduced in accordance with some embodiments of the present invention. As particularly recited in Claim 1:

> A method of message authentication for an SSL-based protocol connection between a source device and a destination device, the method comprising:
>
> **generating a group message authentication code (MAC) based on a plurality of communication packets**, each of the communication packets having at least one data record; and
>
> **transmitting** the plurality of communication packets **using the SSL-based protocol connection** along with the generated group MAC, **wherein ones of the plurality of communication packets do not include an associated packet MAC**.

Applicant submits that at least the highlighted portions of Claim 1 are not disclosed or suggested by the cited references. Independent Claims 26 and 33 contain similar apparatus recitations and Claim 40 includes corresponding computer program product recitations.

Independent Claims 22, 31 and 45 contain receive side recitations corresponding to the transmit side recitations of Claim 1.

In rejecting Claim 1, the Office Action asserts that Gennaro discloses "generating a group MAS [sic] based on a data block" but does not disclose the "data block being broken up into packets." Office Action, p. 2. CSU is relied on as disclosing "breaking data into packets" and Wagner is relied on as disclosing the "use of an SSL based connection to transmit data." Office Action, pp. 2-3. Applicant submits that these rejections overlook the present specification to overly broadly interpret Claim 1 and further rely on a combination of the references that is not supported by the references themselves.

In particular, the present application defines "packet" as:

> Note that, as used herein, a packet may correspond to single data record or may be defined as including a plurality of data records. More particularly, a "packet" corresponds to the record size provided by the SSL-based protocol, or higher layer applications utilizing the SSL-based protocol which impose a different standard, as the maximum number of data records to be transmitted before a corresponding MAC is transmitted under the protocol.

Specification, p. 18, lines 11-16. Thus, as used in Claim 1, a "packet" unit is defined by the SSL-based protocol itself. Accordingly, regardless of whether Gennaro discloses a group MAC or whether CSU discloses breaking data into packets, when combined with the conventional SSL protocol discussion of Wagner the resulting operations would, by definition, not transmit packets with a group MAC without including "an associated packet MAC" with ones of the packets as such a packet MAC inclusion is provided by the SSL protocol of Wagner, as discussed in the present specification. ("As used herein, references to SSL-based protocol refers to protocols, including TLS, where a message authentication code (MAC) is included for each packet and not only to those currently defined protocols referred to as SSL." Specification, p. 12, lines 22-24). Accordingly, the rejection of Claim 1 should be withdrawn for at least these reasons.

Furthermore, Gennaro itself distinguishes its block based digital signature from a MAC. As stated in Gennaro, "[t]his distinguishes digital signatures from *message authentication codes* (MAC) which allow the receiver to have confidence on the identity of the sender, but not to prove to someone else this fact, i.e. MAC's are repudiable."

Gennaro, fn. 1 (italics in original). Gennaro is also particularly directed to handling of message streams. Gennaro, Abstract. Accordingly, the rejection of Claim 1 should also be withdrawn for at least these additional reasons.

Were the rejection to be understood as assuming that the SSL protocol of Wagner would somehow be modified by one of skill in the art in light of Gennaro and CSU to drop packet MACs, such a combination is clearly not suggested by the references. First, as noted above, Gennaro distinguishes its digital signature protocol from a MAC system and, accordingly, would provide no motivation for any such modification to the SSL protocol of Wagner. CSU clearly provides no such motivation as it is directed to memory programming not communication protocols. Finally, Wagner itself favorably compares the SSL 3.0 protocol to SSL 2.0 as "SSL 2.0 uses a weak MAC construction." Wagner, p. 1, Section 2; *see also*, p. 4, Section 3.4 discussing the advantages of the SSL 3.0 MAC protocol. Therefore, if anything, Wagner teaches away from modifying the SSL packet MAC construction. Accordingly, the rejection of Claim 1 should also be withdrawn for at least these additional reasons.

The rejections of Claims 26, 33 and 40 should be withdrawn for similar reasons based on the corresponding recitations therein. Receive side independent Claim 22 includes corresponding recitations related to receiving packets with a group MAC and not including "an associated packet MAC." Accordingly, independent Claims 26, 33 and 45 are also allowable for reasons corresponding to those discussed above with reference to Claim 1.

The dependent claims are patentable at least based on the patentability of the claims from which they depend. In addition, various of the dependent claims are separately patentable. For example, Claims 7-13, 17-19, 29-30, 36 and 43 are separately patentable at least based on the reasons they were found to contain allowable subject matter in the Office Action. Office Action, p. 5.

Claims 2, 27, 34 and 41 include recitations related to a "record count" being communicated corresponding to a number of data records associated with a next group MAC. Claims 23, 32 and 46 contain similar recitations. In rejecting Claims 2, 27, 34 and 41, the Office Action asserts that Gennaro at page 3, bottom of paragraph 3 discloses "transmitting a record count ... indicating a number of data records to be received associtated with a next group MAC." Office Action, p. 3. However, the cited portion of Gennaro merely states "[t]o address the problem of large tables one can also come up with a hybrid scheme in which the stream is split in consecutive pieces and each piece is preceded by a small signed table of contents." The table referred to is a hash table listing cryptographic hashes for the blocks. Applicant submits that this excerpt of Gennaro fails to disclose or suggest the recitations related to a record count number as recited in these respective claims and that these claims are separately patentable for at least these reasons. The claims depending therefrom are similarly separately patentable.

Conclusion

In view of the above, Applicant submits that the pending claims are in condition for allowance and respectfully request allowance of the present application. If further informalities are noted, the Examiner is encouraged to contact the undersigned by telephone to expedite allowance of the present application.

Respectfully submitted,

Robert W. Glatz
Registration No. 36,811

Myers Bigel Sibley & Sajovec, P.A.
Post Office Box 37428
Raleigh, NC 27627
Telephone (919) 854-1400
Facsimile (919) 854-1401